[SG2023-11] 暗号理論の数理と社会実装

暗号理論の基礎

共通鍵暗号の例：Vernam暗号

アリス					ボブ				
平文		鍵		暗号文	暗号文		鍵		平文
1001	⊕ (XOR (mod2の足し算))	0101	=	1100	1100	⊕	0101	=	1001

- バーナム暗号は平文と同じ長さの鍵が必要なので非効率
- 1979年に標準化されたData Encryption Standardは松井さんが1994年に解読
- 2001年に標準化されたAdvanced Encryption Standardは未だに安全
- 共通鍵暗号の最大の欠点は事前に鍵の共有が必要なこと

公開鍵暗号の例：Rivest–Shamir–Adleman暗号

ボブは鍵の組（公開鍵と秘密鍵）を以下の手順でつくる

1. 2つの大きな素数p, qを選び、$N = pq$とする
2. $\gcd(e, (p-1)(q-1)) = 1$を満たすeを選ぶ
3. $ed \equiv 1 \bmod (p-1)(q-1)$を満たす$d$を得る

アリス			ボブ	
平文	公開鍵	暗号文	秘密鍵	平文
$m \in \mathbb{Z}_n$	N, e	$c \equiv m^e \bmod N$	d	$c^d \bmod N (= m)$

- 事前の鍵共有は必要ないが、共通鍵暗号より遅いので、鍵の共有に使われる
- 大きな素数の積の素因数分解が難しいことに基づいて設計されている

耐量子計算機暗号の基礎

耐量子計算機暗号の必要性

- 現在利用されている公開鍵暗号方式は以下の“難しい”問題を利用
  - 大きな素数の積の素因数分解
  - 離散対数問題：$g^x \equiv a \bmod p$を満たすxを見つける
  - 楕円曲線上の離散対数問題
- 量子コンピュータを使うと上記の“難しい”問題が効率的に解ける
  - ショアのアルゴリズム
- 量子コンピュータでも解くのが難しい耐量子計算機暗号の開発が必要不可欠

主な耐量子計算機暗号

- 格子暗号：原点に一番近い格子を見つけることの難しさを利用
  実際に採用されており、現在最も有望な方式
- 多変数多項式暗号：多変数連立2次方程式の求解の難しさを利用
  公開鍵暗号よりも電子署名の方が相性が良い
- 符号ベース暗号：誤り訂正符号の難しさを利用
  格子暗号の下位互換という説もある（？）
- 同種写像暗号：2つの楕円曲線を結ぶ写像を見つけることの難しさを利用
  つい最近、解読方法が見つかってしまった

耐量子計算機暗号の比較

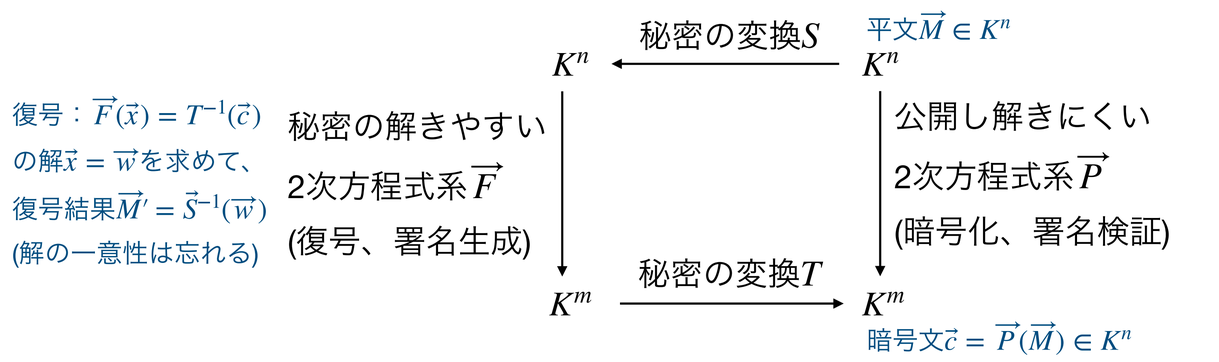
耐量子計算機暗号の公開鍵のサイズなどの比較表

- 耐量子計算機暗号は公開鍵のサイズが非常に大きい
  （同種写像暗号は小さかったが攻撃方法が見つかってしまった）
- 格子暗号の解読方法が見つかってしまったら人類は暗号を失う

耐量子計算機暗号の具体例

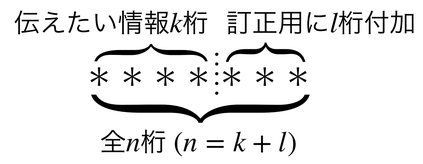
多変数多項式暗号の例：Unbalanced Oil and Vinegar (UOV)

- Kを有限体とし、線型空間K^nの元は列ベクトルで表し、n変数の2次多項式を
  $F_i(\vec{x}) = F(x_1, \ldots, x_n) = \sum_{1 \le j \le k \le n} \alpha_{j,k}^{\langle i \rangle} x_j x_k + \sum_{1 \le j \le n} \beta_j^{\langle i \rangle} x_j + \gamma^{\langle i \rangle}, \quad (\alpha_{j,k}^{\langle i \rangle}, \beta_j^{\langle i \rangle}, \gamma^{\langle i \rangle} \in K, 1 \le i \le m)$
  で与えるとn変数m元連立2次方程式系は$\vec{F}(\vec{x}) := {}^t(F_1(\vec{x}), \ldots, F_m(\vec{x})) = \vec{a}, \ (\vec{a} \in K^m)$
- $\vec{F}$は写像$K^n \to K^m$ともみなせる
- $S\colon K^n \to K^n$と$T\colon K^m \to K^m$を可逆なアフィン変換(1次多項式の写像)とし、
  $\vec{P} = {}^t(P_1, \ldots, P_m) := T \circ \vec{F} \circ S\colon K^n \to K^m$と定めると$\vec{P}$の各成分も2次多項式
- $\vec{F}$は解が得やすい形に選び、S, Tをランダムに選ぶと、$\vec{P}$は求解が困難
- $\vec{P}$を公開し、$\vec{F}, S, T$を秘密にするのが多変数多項式暗号の設計方針
- 解きやすい$\vec{F}$は例えば次のようにしてつくる：
  正整数o, vを$o + v = n$満たすように選び、$F_i(\vec{x})$を次の形にする
  $F_i(\vec{x}) = \sum_{o+1 \le k \le n} \sum_{1 \le j \le k} \alpha_{j,k}^{\langle i \rangle} x_j x_k + \sum_{1 \le j \le n} \beta_j^{\langle i \rangle} x_j + \gamma^{\langle i \rangle}, \quad (\alpha_{j,k}^{\langle i \rangle}, \beta_j^{\langle i \rangle}, \gamma^{\langle i \rangle} \in K)$
  $x_1, \ldots, x_o$に関して連立1次方程式、$x_{o+1}, \ldots, x_{o+v}$を固定すれば容易に求解可能



符号ベース暗号の例：McEliece暗号

誤り訂正符号：線形符号



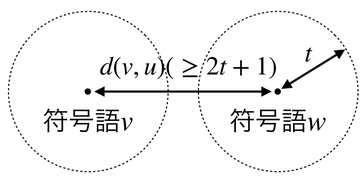
1ビットの誤り訂正の場合
- l桁で誤りの有無と誤りの位置(全n箇所)を検出
- l桁で2^l通り表現できるので$2^l = 1 + n$となる

メッセージ $\in \mathbb{F}_2^k$ ➡ 符号語 $\in C \subset \mathbb{F}_2^n$ ➡ 受信語 $\in \mathbb{F}_2^n$ ➡ 正しい符号語
符号化 with 生成行列$G \in \mathbb{F}_2^{k \times n}$ ／ 通信 ／ 誤り訂正 with パリティ検査行列$H \in \mathbb{F}_2^{l \times n}$

- $[n, k]$-線型符号C：線型空間$\mathbb{F}_2^n$の部分空間で$\dim C = k$のもの（Cの元を符号語とよぶ）
- 生成行列$G \in \mathbb{F}_2^{k \times n}$：行ベクトルが$C$の基底をなす行列、$C = \{uG \mid u \in \mathbb{F}_2^k\}$
- パリティ検査行列$H \in \mathbb{F}_2^{l \times n}$：$C = \{w \in \mathbb{F}_2^n \mid w\,{}^tH = 0\}$を満たす行列（$G\,{}^tH = 0$となる）

最小距離復号

- 最小距離復号：受信語に最も「近い」符号語を選ぶ（ある仮定の下で最も正確な復号法）
- 一般の線形符号に対する最小距離復号はNP困難だが効率的に実行可能な線形符号もある
- Kを有限体とし、一般に線形符号Cは線形空間K^nの部分空間にとる
- ハミング重みwt(v)：$\forall v \in K^n$に対し0でないvの成分の個数
- ハミング距離$d(v, u) :=$ wt$(v - u)$ for $\forall v \in K^n, \forall u \in K^n$、この距離で「近さ」を測る
- Cの最小距離$d_{\min}(C) := \min\{d(v, u) \mid v, u \in C, v \neq u\}$
- Cの誤り訂正能力$t := \left\lfloor \frac{d_{\min}(C) - 1}{2} \right\rfloor$を用いると次がいえる
  $\forall w' \in K^n$に対し$d(w', w) \le t$を満たす符号語$w \in C$は存在すればただ一つ



- 符号語w、受信語w'に対し誤りベクトル$e := w' - w$を導入すると$d(w', w) =$ wt(e)となる

McEliece暗号

- 鍵生成：Kを有限体とし、平文空間は$\mathscr{M} = K^k$、暗号文空間は$\mathscr{C} = K^n$とする
  1. セキュリティパラメータκに応じ、効率的な復号が可能である誤り訂正符号Cを選び、
     Cの生成行列$G_0 \in K^{k \times n}$を作る。復号アルゴリズムをDcd、誤り訂正能力をtとする
  2. 可逆行列$S \in K^{k \times k}$と置換行列$P \in K^{n \times n}$をランダムに選び、$G := SG_0P \in K^{k \times n}$を計算
  3. 公開鍵をpk $= (G, t)$、秘密鍵をsk $= (S, G_0, P,$ Dcd$)$とする
- 暗号化アルゴリズム：平文$m \in \mathscr{M}$とし、wt$(e) = t$を満たす$e \in K^n$をランダムに選び、
  暗号文は$c = mG + e \in K^n$
- 復号アルゴリズム：Dcd$(cP^{-1}) = m'G_0$を解いて$m' \in K^k$を求め、復号は$\tilde{m} = m'S^{-1}$

勝岡さんの研究：多変数連立方程式を1変数化する手法で格子暗号を攻撃